# Active Directory

For an on-premises deployment, three separate Active Directory service accounts must be provided.

## 1. Read-Only Account

This account is used to **query LDAP** for information about users and groups.

- **Role:** `Read-Only`.
- **Function:** Retrieves user and group information via the **LDAP** (or LDAPS) protocol.
- **Required Permissions:** Must have the necessary rights to search and read user attributes in the Active Directory directory.
- **Location in the application:** The credentials for this account will be configured in the Medulla **configuration file** (information requested in the delivery form).

## 2. Machine Enrollment Account (Imaging/Mastering)

This account is dedicated to **provisioning and registering** new machines in the domain during the imaging (or *mastering*) process.

- **Role:** Rights to enroll machines in the domain.
- **Function:** Allow computers to be added to the Active Directory domain.
- **Required Permissions:** Must have the **"Add workstations to the domain"** right **.**
- **Process Integration:** This account will be **integrated and used by** `Sysprep` to perform the domain join operation during machine mastering.

## 3. Script Execution Account (Medulla Agent Installation)

This account is required for post-deployment administration tasks, specifically for**the remote installation of the Medulla agent** via PowerShell, targeting a defined **Organizational Unit (OU)**.

- **Role:** List AD computers and run PowerShell scripts remotely with delegated rights.
- **Function:** List computers in Active Directory. Install and configure the Medulla agent on client machines, targeting machines in a specific OU.
- **Required permissions:**
  - **Delegated Rights on the Target OU:** Must have rights to modify `Computer` objects and rights allowing the execution of remote commands (via **WinRM** or an equivalent solution) on machines in the specified OU.
  - **Access to network share:** If the Medulla agent script or installer is stored on a share, the account must have **read** permissions on that share.
  - **List AD computers: Must**have the right to list AD computers to select the computers on which the agent should be installed.

- **Usage:** This account will be used by the Python application to initiate and validate the execution of PowerShell scripts on the machines, ensuring that the agent is installed and that the machine is correctly assigned to the correct OU structure.

---

Revision #1
Created 2026-04-30 07:36:28 UTC by Adrien Thaissen
Updated 2026-04-30 07:36:28 UTC by Adrien Thaissen